CHAPTER 1
SECTION 1.1

GENERAL ADP REQUIREMENTS

1.0.   GENERAL

1.1.   The TRICARE Systems Manual defines the contractor's responsibilities related to automated processing of health care information and transmission of relevant data between the contractor and TRICARE Management Activity (TMA). It covers three major categories of information flowing among the contractor and TMA/Defense Enrollment Eligibility Reporting System (DEERS): health care coverage information; provider information; and pricing information. For each of these categories it presents specifics of submission, record and data element specifications, editing requirements, and TMA reporting of detected errors to the contractor.

1.2.   This chapter addresses major administrative, functional and technical requirements related to the flow of health care related Automated Data Processing (ADP) information between the contractor and TMA. TRICARE Encounter Data (TED) records as well as provider and pricing information shall be submitted to TMA in electronic media. This information is essential to both the accounting and statistical needs of TMA in management of the TRICARE program and in required reports to Department of Defense, Congress, other governmental entities, and to the public. Technical requirements for the transmission of data between the contractor and TMA are presented in this section. The requirements for submission of TRICARE Encounter Data records and resubmission of records are outlined in Chapter 2, Section 1.1, the TMA requirements related to submission and updating of provider information are outlined in Chapter 2, Section 1.2 and the TMA requirements related to submission and updating of pricing information are outlined in Chapter 2, Section 1.3.

1.3.   The ADP requirements shall incorporate the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandated standards where required.

2.0.   ADP REQUIREMENTS

It is the responsibility of the contractor to employ adequate hardware, software, personnel, procedures, controls, contingency plans, and documentation to satisfy TMA data processing and reporting requirements. Items requiring special attention are listed below.

2.1.   Continuity of Operations Plan (COOP)

2.1.1.   The contractor shall develop a plan to ensure the continuous operation of their information technologies (IT) systems and data support of TRICARE. The COOP shall ensure the availability of the system and associated data in the event of hardware, software and/or communications failures. The contractor shall develop a COOP that will enable compliance

with all processing standards as defined in the TRICARE Operations Manual, Chapter 1, Section 3.

2.1.2. The contractor shall conduct a test of the backup system within the first quarter of the initial health care delivery period and shall continue to assure backup capabilities by testing or reviewing the availability and capability of the backup ADP system to process the TRICARE data and produce the expected results. The contractor's testing of the backup system shall be done at least once a year.

2.1.3. Annual disaster recovery tests shall involve a total of 400 claims and be performed in two parts. Contractors shall perform claims and catastrophic inquiries for 200 claims against production DEERS and the production Catastrophic Cap and Deductible Database (CCDD) on DEERS. This test will demonstrate the ability to connect to production DEERS and the CCDD from the recovery site and the ability to successfully submit claims inquiries and receive DEERS claims responses and Catastrophic Cap Inquiries and responses. Contractors shall <u>not</u> perform catastrophic cap updates in the CCDD and DEERS production regions for these 200 test claims.

2.1.4. To successfully demonstrate the ability to perform catastrophic cap updates and to create newborn placeholder records on DEERS the contractor shall process an additional 200 claims using the DEERS and CCDD contractor test region. Contractors shall coordinate connectivity to the DEERS and the CCDD production and contractor test regions with DMDC at least 30 days prior to the test. In all cases, the results of the review and/or test results shall be reported to the TMA, Contract Management Division within 15 days of conclusion of the review or test.

2.2. DoD Information Technology Security Certification And Accreditation Process (DITSCAP) Requirements

Contractor Information Systems (IS)/networks involved in the operation of systems of records in support of the DoD Military Health System requires obtaining, maintaining, and using sensitive and personal information strictly in accordance with controlling laws, regulations, and DoD policy.

2.2.1. The contractor's IS/networks involved in the operation of DoD systems of records shall be safeguarded through the use of a mixture of administrative, procedural, physical, communications, emanations, computer and personnel security measures that together achieve the same requisite level of security established for DoD IS/networks for the protection of information referred to as "Sensitive Information" (SI) and/or "Controlled Unclassified Information." The contractor shall provide a level of trust which encompasses trustworthiness of systems/networks, people and buildings that ensure the effective safeguarding of SI against unauthorized modifications, disclosure, destruction and denial of service.

2.2.2. Information System (IS)/Networks Certification and Accreditation (C&A)

The contractor's IS/networks shall comply with the C&A process established under the DITSCAP for safeguarding SI accessed, maintained and used in the operation of systems of records under this contract.

2.2.3. **Certification And Accreditation (C&A) Process**

The C&A process ensures that the trust requirement is met for systems and networks. Certification is the determination of the appropriate level of protection required for IS/networks. Certification also includes a comprehensive evaluation of the technical and nontechnical security features and countermeasures required for each system/network. Accreditation is the formal approval by the government to operate the contractor's IS/ networks in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. In addition, accreditation allows IS/networks to operate within the given operational environment with stated interconnections; and with appropriate level of protection for the specified period. The C&A requirements apply to all DoD IS/networks and contractor's IS/networks that access, manage, store, or manipulate electronic SI data.

2.3. The DITSCAP is the standardized approach to the certification and accreditation (C&A) process within DoD. Each IS/network that undergoes DITSCAP must have required security controls in place, must have documented the security components and operation of the IS/network and must successfully complete testing of the required security controls. The contractor shall ensure DITSCAP documentation is available for review and is accurate. The contractor shall also implement an information assurance vulnerability management program providing mitigation from known vulnerabilities. The contractor, as part of that program, shall provide a primary and secondary point of contact for the MHS Information Assurance Vulnerability Alert (IAVA) Monitor. The point of contact shall provide, upon receipt of a vulnerability message, an acknowledgment of receipt. The contractor shall mitigate the vulnerability, and upon mitigation, report compliance. Receipt and compliance messages to the government shall occur within the stipulated window, as stated in the vulnerability message, and be directed to the MHS IAVA Monitor. Mitigation compliance for IA vulnerabilities shall be assessed on an annual basis.

The contractor shall execute the DITSCAP process by providing, for receipt by the Contracting Officer within 30 days following contract award, the required documentation necessary to receive an Approval to Operate (ATO), and making their IS/networks available for testing. The contractor shall be required to mitigate the vulnerabilities identified for correction during the risk assessment process. The above requirements shall be met before interconnecting with any DoD IS/network is authorized. The Military Health System (MHS) DITSCAP Checklist is provided for assistance regarding meeting the DITSCAP requirements. Reference material and DITSCAP tools can be obtained at http://www.tricare.osd.mil/ tmis_new/ia.htm.

3.0. **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)**

The contractor shall be compliant with the Health Insurance Portability and Accountability Act (HIPAA) as implemented by the Department of Health and Human Services (DHHS) final rule on Health Insurance Reform: Security Standards (45 Code of Federal Regulations, Parts 160, 162, and 164), effective April 21, 2003. Although the compliance date established by the DHHS final rule is April 21, 2005, the contractor shall be in compliance with the requirements of the final rule at the start-work date of this contract.

4.0.   PHYSICAL SECURITY REQUIREMENTS

The contractor shall employ physical security safeguards for IS/networks involved in the operation of its systems of records to prevent the unauthorized access, disclosure, modification, destruction, use, etc., of SI and to otherwise protect the confidentiality and ensure the authorized use of SI. In addition, the contractor shall support a Physical Security Audit performed by the government of its internal information management infrastructure using the criteria from the Physical Security Audit Matrix. The contractor shall correct any deficiencies identified by the government of its physical security posture. The Physical Security Audit Matrix can be accessed via the Policy and Guidance/Security Matrices section at http://www.tricare.osd.mil/tmis_new/ia.htm.

5.0.   PERSONNEL SECURITY ADP/IT REQUIREMENTS

5.1.   Policy References

Personnel to be assigned to an ADP/IT position must undergo a successful security screening before being provided access to DoD information technology (IT) resources. Prior to an employee being granted interim access to DoD sensitive information, the organization must receive notification that the Office of Personnel Management (OPM) has scheduled the employee's investigation. The references and specific guidance below provided to TMA by the Under Secretary of Defense for Intelligence (USDI) and OPM safeguard against inappropriate use and disclosure.

- Privacy Act of 1974

- Health Insurance Portability and Accountability Act (HIPAA) of 1996

- DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 2003

- DoD 5200.2-R, "Personnel Security Program," (January 1987)"

- DoD 5220.22-M, "National Industrial Security Program Operating Manual" (NISPOM), January 1995 (Change 2, May 1, 2000)

- DoDI 8500.1, "Information Assurance (October 24, 2002)."

The requirement above must be met by contractors, subcontractors and others who have access to information systems containing information protected by the Privacy Act of 1974 and protected health information under HIPAA. Background checks are required for all ADP/IT personnel who receive, process, store, display, or transmit sensitive information (SI).

5.2.   Formal Designations Required

All contractor personnel in positions requiring access to DoD IS/networks or COCO IS/networks interconnected with DoD IS/networks must be designated as ADP/IT-I, ADP/IT-II, or ADP/IT-III. Only TRICARE contractors are permitted to submit ADP/IT background checks in accordance with this policy. Military Service and Military Treatment Facility contractors are not to use this guidance.

5.3.   Special Access Requirements

All contractor personnel accessing the Defense Enrollment Eligibility Reporting System (DEERS) database or the Business to Business (B2B) Gateway must have an ADP/IT-II Trustworthiness Determination. Contractor personnel currently working in DEERS with an ADP/IT-III or an interim ADP/IT-III Trustworthiness Determination must upgrade to an ADP/IT-II or interim ADP/IT-II Trustworthiness Determination no later than October 1, 2004. DEERS access for contractor personnel with ADP/IT-III Trustworthiness Determinations will no longer be granted after October 1, 2004.

New employees hired by contractors are granted interim access for six months upon submission of the SF 85P and fingerprint cards to the Office of Personnel Management. Contractors must notify the TMA Privacy Office of the submission of SF 85Ps for new hires and the date submitted. In addition, Contractors are required to respond timely to the Office of Personnel Management for requests for additional information required for the processing of the SF 85P. Failure to respond timely to the Office of Personnel Management will result in the revocation of interim access by the TMA Privacy Office.

Contractors are required to ensure personnel viewing data obtained from DEERS or the B2B Gateway or viewing Privacy Act protected data follow contractor established procedures as required by the TRICARE Operations Manual, Chapter 1, Section 4, paragraph 3.0., to assure confidentiality of all beneficiary and provider information. The contractor is required to assure the rights of the individual are protected in accordance with the provisions of the Privacy Act, HIPAA and HHS Privacy regulation and to prevent the unauthorized use of TMA files.

5.4.   ADP/IT Category Guidance

In establishing the categories of positions, a combination of factors may affect the determination. Unique characteristics of the system or the safeguards protecting the system permit position category placement based on the agency's judgement. Guidance on ADP/IT categories is:

ADP/IT-I - Critical Sensitive Position. A position where the individual is responsible for the development and administration of MHS IS/network security programs and the direction and control of risk analysis and/or threat assessment. The required investigation is equivalent to a Single-Scope Background Investigation (SSBI). Responsibilities include:

- Significant involvement in life-critical or mission-critical systems.

- Responsibility for the preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting severe damage to persons, properties or systems, or realizing significant personal gain.

- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater; (2) lesser amounts if the activities of the individuals are not subject to technical review by higher authority in the ADP/IT-I category to insure the integrity of the system.

- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring and or management of systems hardware and software.

- Other positions as designated by the DAA that involve a relatively high risk for causing severe damage to persons, property or systems, or potential for realizing a significant personal gain.

ADP/IT-II - Non-critical-Sensitive Position. A position where an individual is responsible for systems design, operation, testing, maintenance and/or monitoring that is carried out under technical review of higher authority in the ADP/IT-I category, includes but is not limited to: (1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, or Government-developed privileged information involving the award of contracts; (2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year.

Other positions are designated by the DAA that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP/IT-I positions. The required investigation is equivalent to a National Agency Check with Law Enforcement and Credit (NACLC).

ADP/ITs submitted as a NAC to DSS prior to 2000 were approved as ADP/IT-II/III. Effective 2000, OPM took over the investigation process for TMA. The submission requirements for ADP/IT levels were upgraded as follows: ADP/IT-III is a NAC; ADP/IT-II is a NACLC and; an ADP/IT-I is a SSBI. Investigations submitted before 2000 for a NAC (ADP/IT-II/III) will need to submit a new SF85P User Form and fingerprint card for a NACLC to be upgraded to an ADP/IT-II.

ADP/IT-III - Non-sensitive Position. All other positions involved in Federal computer activities. The required investigation is equivalent to a National Agency Check (NAC).

5.5. Additional ADP/IT Level Designation Guidance

All TMA contractors requiring ADP/IT-I Trustworthiness Determinations for their personnel are required to submit a written request for approval to the TMA Privacy Office prior to submitting applications to OPM. The justification will be submitted to the TMA Privacy Officer, Skyline Five, 5111 Leesburg Pike, Suite 810, Falls Church, Virginia, 20041, on the letterhead of the applicant's contracting company. The request letter must be signed by, at a minimum, the company security officer or other appropriate executive, include contact information for the security officer or other appropriate executive, and a thorough job description which justifies the need for the ADP/IT-I Trustworthiness Determination. Contractors shall not apply for an ADP/IT-I Trustworthiness Determination unless specifically authorized by the TMA Privacy Officer.

5.5.1. Required Forms

Each contractor shall be required to complete and submit the necessary standard forms, fingerprint forms, and other documentation as may be required by the Office of

Personnel Management (OPM) to open and complete investigations. Additional information may be requested while the investigation is in progress. This information must be provided in the designated timeframe or the investigation may be closed. All contractor employees that are prior military should include Copy 4 of the DD214 (certificate of Release or Discharge from Active Duty) with their original submission. Forms and guidance can be found at http://www.opm.gov/extra/investigate.

NOTE: The appropriate billing code will be provided following contract award. Contractors should contact the TMA Privacy Office to obtain the PIPS Form 12 when applying for a Submitting Office Number (SON). The application and billing information must be requested from the TMA Privacy Office. Each contracting company or subcontracting company must contact the TMA Privacy Office individually for this information.

5.5.2.   Interim Assignment: (U.S. Citizens Working In The U.S. Only)

Contractor personnel who are U.S. Citizens will receive an OPM Investigation Schedule Notice (ISN) from the TMA Privacy Office once the Office of Personnel Management (OPM) has scheduled the investigation. TMA sends the ISN to the contracting security officer as validation for interim access. The contractor security officer may use receipt of the ISN as their authority to grant interim access to DoD IS/networks until a Trustworthiness Determination is made.

Contractor personnel undergoing the process to upgrade their current Trustworthiness Determination level (e.g., ADP/IT-III to ADP/IT-II) who maintain continuous employment with the contractor, or have had no lapse in employment with the contractor of greater than 24 months, shall continue to have the current access level during the upgrade process.

5.5.3.   Temporary Assignments (U.S. Citizens Only)

Temporary employees include intermittent, volunteers, and seasonal workers. Efforts shall be taken to obtain an approved ADP/IT-II or ADP/IT-III Trustworthiness Determination for those positions requiring access to DoD sensitive information. Interim access is allowed as outlined in paragraph 5.5.2. above.

5.5.4.   Preferred/Partnership Providers At OCONUS MHS Facilities (U.S. Citizens Only)

To obtain an ADP Trustworthiness Determination for a preferred/partnership provider the Security Officer of the MTF will contact the TMA Privacy Officer for instructions and guidance on completing and submitting the SF85P User Form, fingerprint cards and system access. The TMA Privacy Officer will provide guidance on system access upon contact by the Security Officer of the MTF.

5.5.5.   ADP/IT Level Trustworthiness Determination Upgrades

Contact the TMA Privacy Office if a higher ADP/IT level is required than what was submitted for an employee. In addition, the contractor's security officer must contact the OPM Federal Investigations Processing Center to determine the status of the investigation.

OPM can upgrade the level of investigation only if the investigation has not been closed/completed. If the NAC is pending, you may fax a request to upgrade the NAC to a NACLC in writing to OPM, Attention: Corrections Technician. You must provide the name, SSN, and Case Number on your request (Case Number can be found on the ISN). If the SF85P User Form is missing information, the Correction Technician will call the requester for missing information. Addresses for each organization are shown below.

- TMA Privacy Office, Skyline Five, 5111 Leesburg Pike, Suite 810, Falls Church, Virginia, 22041

- OPM Federal Investigations Processing Center, P.O. Box 618, Boyers, Pennsylvania, 16018-0618

- OPM Corrections Department, Federal Investigations Processing Center, P.O. Box 618, Boyers, Pennsylvania, 16018-0618

If the investigation has been closed/completed, the original SF85P Agency User Form (coversheet) must be submitted for the higher ADP/IT level. The SF85P may be re-used within 120 days of the case closed date, with corrected ADP level code (ADP/IT-II=O8B). The letter "I" must be inserted in the Codes box located above C and D on the SF85P Agency User Form and no fingerprint card is needed. The contractor's Security Officer must update the SF85P Agency User Form, re-sign and re-date the form in Block P. The individual must line through any obsolete information, replacing it with corrected information and initial all changes made to the SF85P. The individual must the re-sign and re-date the certification section of the form.

If it is beyond the 120 day period, the old SF85P may be used if all the information is updated and the certification part of the form is re-dated, and re-signed by the individual. A new SF85P Agency User Form (coversheet) showing the correct ADP/IT (O8B) level code is required at this time. Each correction/change made to the form must be initialed and dated by the individual. Fingerprint cards must be submitted if the case has been closed for more than 120 days.

5.6. Assignment Of Non-U.S. Citizens

5.6.1. Policy

Interim Access at CONUS locations for Non-U.S. Citizens is Not Authorized. Non-U.S. citizen contractor employees are not being adjudicated for any Trustworthiness positions.

5.6.2. Grandfathering Of Non-U.S. Citizens

Earlier guidance authorized the grandfathering (continuation) of certain CONUS non-U.S. Citizens who previously were working on a TMA contract. Grandfathered contractor personnel are authorized to continue working under the existing contract until contract expiration date. This provision is not applicable to contractor employees who opt to transition employment from a contractor holding a legacy TRICARE contract to a contractor awarded a contract under the TRICARE Next Generation series of contracts.

5.6.3.   **End Date Of CONUS Non-U.S. Citizen Access**

Access to DoD IS/networks or data will end on December 31, 2004 for all CONUS non-U.S. Citizen contractor personnel, or in accordance with the guidance provided in paragraph 5.6.2.

5.6.4.   **Non-U.S. Citizens/Foreign Nationals Working At OCONUS MHS Facilities**

Non-U.S. Citizens/Foreign Nationals employed by DoD organizations overseas, whose duties do not require access to classified information, shall be the subject of record checks that include host-government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government, initiated by the appropriate Military Department investigative organization prior to employment.

5.7.   **Transfers Between Contractor Organizations**

5.7.1.   When contractor employees transfer employment from one government contractor to another, while their investigation for ADP/IT Trustworthiness Determination is in process, the investigation being conducted for the previous employer may be applied to the new employing contractor. The new contracting company will send an Excel spreadsheet to the TMA Privacy Office to provide notification of the addition of the new employee from a previous TRICARE contractor. The spreadsheet must contain the following:

- Name
- Social Security Number
- Name of the former employing contractor
- ADP/IT level applied for
- Effective date of the transfer/employment

TMA will verify the status of the Trustworthiness Determination/scheduled investigation for the employee(s) being transferred. If the investigation has not been completed, the TMA Privacy Office will notify OPM to transfer the investigation from the old SON (submitting office number) to the new SON. If the investigation has been completed, OPM cannot affect the transfer. If the Trustworthiness Determination has been approved, TMA will verify the approval of the Trustworthiness Determination and send a copy to the new employing contractor's office.

5.8.   **New Contractor Personnel With Recent Secret Clearance**

New contractor personnel who have had an active secret clearance within the last two years do not need to submit a SF85P User Form. The contracting company will need to send a copy of the Letter of Consent (LOC) to the TMA Privacy Office for verification.

5.9.   **Notification Of Submittal And Termination**

Contracting companies must notify the TMA Privacy Office when the Security Officer has submitted the SF85P User Form to OPM for new employees. Upon termination of

a contractor employee from the TRICARE Contract, contracting companies must notify the TMA Privacy Office and OPM of the action, including the termination date.

5.10.   Exception Or Extensions

Exceptions to or extensions beyond any end date or other requirement will be granted (if approved) only by the Director, TRICARE or the Deputy Director, TRICARE. Any exception or extension, if provided, will be in response to a written request, and based upon appropriate health program interests.

6.0.   PUBLIC KEY INFRASTRUCTURE (PKI)

The DoD has initiated a Public Key Infrastructure policy to enhance the identification and authentication of users and systems within DoD. The PKI program is in its initial stage and is evolving. The following paragraphs provide current DoD PKI requirements. Additional guidance as it applies to this contract will be provided as the policy and implementation guidance is finalized within DoD.

The contractor is required to obtain PKI certificates for individuals who will be directly accessing any DoD applications which reside either on a DoD Local Area Network or a DoD private (restricted access, e.g., username/password) Web server including, but not limited to, the following:

- The Defense Online Enrollment System (DOES) [DEERS client/server application]
- The General Inquiry of DEERS (GIQD) application [DEERS Web application]
- The TRICARE Duplicate Claims System [TMA Web application]
- The Enterprise Wide Referral and Authorization System (EWRAS) [Web application]
- Civilian PCM Panel Reassignment [DEERS Client/Server application]
- Catastrophic Cap and Deductible/Fee Research [DEERS Web application]
- PCM Research [DEERS Web application]
- DEERS Security Web Application [Web application]
- OHI/SIT [DEERS Web application]
- Direct Care PCM Panel Reassignment [Web application]
- Purchased Care [Web application]

Contractor personnel who access these systems from a .mil domain will be eligible to receive their certificates from the government. PKI certificates for contractor personnel that access the above listed systems from non-.mil domains may be purchased through DoD approved External Certification Authorities (ECAs).

Additionally the contractor is required to obtain DoD acceptable PKI server certificates for identity and authentication of the servers involved in the following system-to-

system or host-to-host interfaces. These interfaces include, but are not limited to, the following:

- Contractor systems for claims eligibility inquiries and responses and DEERS

- Contractor systems and the TRICARE Encounter Data (TED) Processing Center

7.0. TELECOMMUNICATIONS

7.1. MHS Demilitarized Zone (DMZ) Managed Partner Care Business To Business (B2B) Gateway

7.1.1. All contractor systems that will communicate with DoD systems will interconnect through the established MHS B2B gateway. For all Web applications, contractors will connect to a DISA-established Web DMZ.

7.1.2. In accordance with contract requirements, MCS contractors will connect to the B2B gateway via a contractor procured Internet Service Provider (ISP) connection. Contractors will assume all responsibilities for establishing and maintaining their connectivity to the B2B Gateway. This will include acquiring and maintaining the circuit to the B2B Gateway and acquiring a Virtual Private Network (VPN) device compatible with the MHS VPN device.

7.1.3. It is anticipated that modifications will also allow provisioning of dedicated point-to-point commercial circuits to the B2B gateway. The DISA B2B Gateway is a redundant service that is provisioned at two locations. If contractors require high availability, they may acquire redundant circuits to both locations.

7.1.4. Contractors will comply with DoD guidance regarding allowable ports, protocols and risk mitigation strategies.

7.2. Contractor Provided IT Infrastructure

7.2.1. Platforms shall support HTTP, HTTPS, Web derived Java Applets, client/server, FTP, secure FTP, and all software that the contractor proposes to use to interconnect with DoD facilities.

NOTE: The DoD is phasing out the use of FTP. Upon notification from the government, the contractor shall cease using FTP and begin utilizing the FTP alternative stipulated by the government.

7.2.2. Contractors shall configure their networks to support access to government systems (e.g., configure ports and protocols for access).

7.2.3. Contractors shall provide full time connections to a TIER 1 or TIER 2 ISP. Dial-up ISP connections are not acceptable.

7.3.   Defense Information System Agency (DISA) Form 41 Submission

All contractors that use the DoD gateways to access government systems must submit a DISA Form 41 or equivalent in accordance with Contracting Officer guidance. In addition, Form 41s are required for each system administrator responsible for each host-to-host interface. Contractors shall complete and submit to TMA one Form 41 for their organization, attached to which shall be a listing of those individuals for whom background checks have been completed or for whom requests/applications for background checks have been completed, submitted to the Office of Personnel Management (OPM), and acknowledgements have been received from OPM that the applications are complete and are pending action by OPM. The request must clearly delineate the ports and protocols used for each IP address. The contractor shall complete the form and submit it to the government for final processing.

7.4.   MHS Systems Telecommunications

7.4.1.   The primary communication links shall be via Secure Internet Protocol (IPSEC) virtual private network (VPN) tunnels between the contractor's primary site and the MHS B2B Gateway.

7.4.2.   The contractor shall place the VPN appliance device outside the contractor's firewalls and shall allow full management access to this device (e.g., in router access control lists) to allow Central VPN Management services provided by the Defense Information Systems Agency (DISA) or other source of service as designated by the MHS to remotely manage, configure, and support this VPN device as part of the MHS VPN domain.

7.4.3.   For backup purposes, an auxiliary VPN device for contractor locations shall also be procured and configured for operation to minimize any downtime associated with problems of the primary VPN.

7.4.4.   The MHS VPN management authority (e.g., DISA) will remotely configure the VPN once installed by the contractor.

7.4.5.   Maintenance and repair of contractor procured VPN equipment shall be the responsibility of the contractor. Troubleshooting of VPN equipment shall be the responsibility of the government.

7.5.   Contractors Located On Military Treatment Facilities (MTFs)

7.5.1.   If the contractor plans to locate personnel on a military facility, the contractor must coordinate with the Base/Post/Camp communications office and the MTF.

7.5.2.   Contractors located on military facilities who require direct access to government systems shall coordinate/obtain these connections with the local MTF and Base/Post/Camp communication personnel. These connections will be furnished by the government.

7.5.3.   Contractors located on military facilities that require direct connections to their networks shall either:

- Coordinate their network connections to the respective military infrastructure and through the MHS B2B Gateway.

- If the contractor requires a direct connection back to the contractor's network, they shall provide an isolated IT infrastructure, coordinate with the Base/ Post/Camp communications personnel and the MTF in order to get approval for a contractor procured circuit to be installed and to ensure the contractor is within compliance with the respective organizational security policies, guidance and protocols. Note: In some cases, the contractor may not be allowed to establish these connections due to local administrative/security requirements.

7.5.4.   The contractor shall be responsible for all security certification documentation as required to support DoD Information Assurance requirements for network interconnections. Further, the contractor shall provide, on request, detailed network configuration diagrams to support DITSCAP accreditation requirements. The contractor shall comply with DITSCAP accreditation requirements. All network traffic shall be via TCP/IP using ports and protocols in accordance with current Service security policy. All traffic that traverses MHS, DMDC, and/or military Service Base/Post/Camp security infrastructure is subject to monitoring by security staff using Intrusion Detection Systems.

7.6.   **DEERS**

7.6.1.   **Primary Site**

7.6.1.1.   The DEERS primary site is located in Auburn Hills, Michigan and the backup site is located in Seaside, California.

7.6.1.2.   The contractor shall communicate with DEERS through the MHS B2B Gateway.

7.6.2.   **PCs/Hardware**

          The contractor is responsible for all systems and operating system software needed internally to support the DOES.

7.7.   **TMA/TRICARE Encounter Data**

7.7.1.   **Primary Site**

          The TRICARE Encounter Data (TED) primary site is currently located in Denver, Colorado, and operated by the Defense Enterprise Computing Center (DECC), Denver Detachment for the DISA. Note: The location of the primary site may be changed. The contractor shall be advised should this occur.

7.7.2.   General

The common means of administrative communication between Government representatives and the contractor is via telephone and e-mail. An alternate method may be approved by TMA, as validated and authorized by TMA. Each contractor on the telecommunication network is responsible for furnishing to TMA at the start-up planning meeting (and update when a change occurs), the name, address, and telephone number of the person who will serve as the technical point of contact. Contractors shall also furnish a separate computer center (Help Desk) number to TMA which the TMA computer operator can use for resolution of problems related to data transmissions.

7.7.3.   TED-Specific Data Communications Technical Requirements

7.7.3.1.   Systems Interface Requirements

The contractor shall communicate with the government's Data Center through the MHS B2B Gateway.

7.7.3.2.   Communication Protocol Requirements

7.7.3.2.1.   File transfer software shall be used to support communications with the TED Data Processing Center. CONNECT:Direct is the current communications software standard for TED transmissions. The contractor is expected to upgrade/comply with any changes to this software. The contractor shall provide this product and a platform capable of supporting this product with the TCP/IP option included. Details on this product can be obtained from:

> Sterling Commerce
> 4600 Lakehurst Court
> P.O. Box 8000
> Dublin, OH 43016-2000 USA
> http://www.sterlingcommerce.com/solutions/products/ebi/connect/direct.html
> Phone: 614-793-7000
> Fax: 614-793-4040

7.7.3.2.2.   For Ports and Protocol support, TCP/IP communications software incorporating the TN3270 emulation shall be provided by the contractor.

7.7.3.2.3.   Transmission size is limited to any combination of 250,000 records at one time.

7.7.3.2.4.   "As Required" Transfers

Ad hoc movement of data files shall be coordinated through and executed by the network administrator or designated representative at the source file site. Generally speaking, the requestor needs only to provide the point of contact at the remote site, and the source file name. Destination file names shall be obtained from the network administrator at the site receiving the data. Compliance with naming conventions used for recurring automated transfers is not required. Other site specific requirements, such as security constraints and pool names are generally known to the network administrators.

7.7.3.2.5.   File Naming Convention

7.7.3.2.5.1.   All files received by and sent from the TMA data processing site shall comply with the following standard when using CONNECT:Direct:

POSITION(S)	CONTENT
1 - 2	'TD'
3 - 8	YYMMDD Date of transmission
9 - 10	Contractor number
11 - 12	Sequence number of the file sent on a particular day. Ranges from 01 to 99. Reset with the first file transmission the next day.

7.7.3.2.5.2.   All files sent from the TMA data processing site shall be named after coordination with receiving entities in order to accommodate specific communication requirements for the receivers.

7.7.3.2.5.3.   Timing

Telecommunication transfers during normal business hours may be adversely affected by normal processing. Therefore, every attempt shall be made to maximize utilization of telecommunications lines by deferring transfers to night-time operation. Ideally, a single file will be transmitted at night. However, there are no restrictions on the number of files that may be transmitted. Under most circumstances, the source file site shall initiate automated processes to cause transmission to occur. With considerations for timing and frequency, activation of transfers for each application shall be addressed on a case by case basis.

7.7.3.2.5.4.   Alternate Transmission

Should the contractor not be able to transmit their files through the normal operating means, the contractor should notify TMA (EL/DS Operations) that they will be sending their files by tape via overnight delivery.

7.8.   TMA/MHS Referral And Authorization System

7.8.1.   Primary Site

The MHS Referral and Authorization System primary site is to be determined.

7.8.2.   PCs/Hardware

The contractor is responsible for all systems and operating system software needed internally to support the MHS Referral and Authorization System.

7.9.   TMA/TRICARE Duplicate Claims System

7.9.1.   Primary Site

The TRICARE Duplicate Claims System (DCS) primary site is located in Aurora, Colorado.

7.9.2.   Contractor Connection With TMA For The Duplicate Claims System (DCS)

The DCS is planned to operate as a web application. The contractor is responsible for providing internal connectivity to the public Internet. The contractor is responsible for all systems and operating system software needed internally to support the DCS. (See the TRICARE Operations Manual, Chapters 9 and 10 for DCS Specifications.)